FlipIt

Simon Forest Baptiste Lefebvre Vincent Vidal

April 19, 2013

Abstract

Ideal cryptography systems are based on a secret, a key, however advanced Persistent Threat (APT) have undermined secure protocols. *FlipIt* [1], [2] is a recent two-player game between an attacker and defender. It provides a simple and elegant framework to formalize their interactions and allows the description of pratical threats.

We propose a variant of FlipIt, a two-player game where players compete to control a shared ressource. Players can move at any given time, taking control of the ressource. However the identity of the player controlling the ressource is not revealed until a player actually moves. We consider that the average move rate by player is bounded, the number of moves made by player up to an including time can not be greater than a constant times this time.

First we introduce formal definitions and notation in order to make an exhaustive description of our variant of FliIt.

`[Describe here the end of the structure of this article]`

`[Describe here the results of this article]`

1 Formal Definition and Notation

This section gives a formal definition of the variant of FlipIt.

Players There are two players identified with 0 and 1. Keep the game symetric between the two players will be useful for our studies.

Time The game begins at time $t = 0$ and continues indefinitely. It is viewed as being continuous.

Game state $C(t)$ denotes the current player controlling the ressource at time t, $C(t)$ is either 0 or 1. For $i = 0, 1$ let $C_i(t) = 1_{\{C(t)=i\}}$ two *indicator functions*.

Moves A player may *flip the ressource* or *move* at any time, but he is not allowed to exceed a fixed *average move rate*. A player cannot move more than once at a given time. If different players play at the same time then the moves *cancel* and everything goes such as nothing happened. We introduce the following notations:

$$\mathbf{t} = t_0\, t_1\, \ldots\, t_n\, \ldots$$

denotes the *sequence of moves times by both players*,

$$\mathbf{n}(t) = \mathrm{Card}\{t_n : t_n \leq t\}$$

denotes the *number of moves made by both players up to an including time* t,

$$\boldsymbol{\alpha}(t) = \frac{\mathbf{n}(t)}{t}$$

denotes the *average move rate by both players*. We can define notations for same entities only for one player, let consider player i:

$$\mathbf{t}_i = t_{i,0}\, t_{i,1}\, \ldots\, t_{i,n}\, \ldots \qquad \mathbf{n}_i(t) = \mathrm{Card}\{t_{i,n} : t_{i,n} \leq t\} \qquad \boldsymbol{\alpha}_i(t) = \frac{\mathbf{n}_i(t)}{t}$$

denote the *sequence of moves times by player* i, the *number of moves made by players* i *up to an including time* t, denotes the *average move rate by player* i.

Rule For a given player i let $\mathbf{A}_i \in \mathbf{R}^+$ denotes the *average move rate upper bound for player* i. The moves of this player have to verify at any time t:

$$\boldsymbol{\alpha}_i(t) \leq \mathbf{A}_i$$

Which means that a player capitalized time into opportunities to play.

Gain For a given game at any time t:

$$\mathbf{G}_i(t) = \int_0^t \mathbf{C}_i(u)\,\mathrm{d}u$$

denotes the *total gain by player* i *up to time* t which is not really convenient for our studies. We introduce another metric:

$$\boldsymbol{\gamma}_i(t) = \frac{\mathbf{G}_i(t)}{t}$$

which denotes the *average gain rate for player* i *up to time* t and leads to the value:

$$\boldsymbol{\Gamma}_i = \lim_{t \to +\infty} \boldsymbol{\gamma}_i(t)$$

This *average gain rate for player* i will found our game's strategy comparisons.

2 Playing periodically

We assume here that both players have a periodic strategy.Let φ_i and α_i the phase and the period of the player i. So, we have for each n,

$$t_{i,n} = \varphi_i + n.\alpha_i$$

We can assume that $\alpha_0 \leq \alpha_1$. As the average gain rate doesn't depend of the initial time, we can assume that $\varphi_0 = 0$ too. Let $\Gamma(\alpha_0,\, \alpha_1,\, \varphi_1)$ be the average gain rate for the player 0. It's easy to sea that :

$$\Gamma(\alpha_0,\, \alpha_1,\, \varphi_1) = \Gamma\left(1,\, \frac{\alpha_1}{\alpha_0},\, \frac{\varphi_1}{\alpha_0}\right)$$

A faire :
`Dessin et explication pour arriver à la formule`

$$\Gamma(1,\,\alpha,\,\varphi) = \lim_{N\to+\infty}\frac{1}{N}\sum_{\substack{n\geq 0\\ \alpha n+\varphi<N}}(1-\mathrm{frac}\,(\alpha n+\varphi_0)) = \frac{1}{\alpha}-\frac{1}{\alpha}\lim_{N\to+\infty}\frac{1}{N/\alpha}\sum_{n=0}^{N/\alpha}\mathrm{frac}\,(\alpha n+\varphi_0)$$

So, we have :

$$\Gamma(1,\,\alpha,\,\varphi_0) = \frac{1}{\alpha}-\frac{1}{\alpha}\lim_{N\to+\infty}\frac{1}{N}\sum_{n=0}^{N}\mathrm{frac}\,(\alpha n+\varphi_0)$$

Then, it's easy to calcul the average gain rate.

For the first case, we assume that $\alpha = \frac{p}{q}+r \in \mathbf{Q}$ where $\mathrm{pgcd}\,(p,\,q)=1$ and $p<q$. Because p and q are co-prime integers, the two set $[\![0,\,q-1]\!]$ and $\{p.n\ [\mathrm{mod}\,q]\ n\in[\![0,\,q-1]\!]\}$ are equal. We can conclude that :

$$\sum_{n=0}^{q-1}\mathrm{frac}\left(\left(\frac{p}{q}+r\right)n\right) = \sum_{n=0}^{q-1}\mathrm{frac}\left(\frac{p}{q}n\right) = \sum_{n=0}^{q-1}\frac{(p.n\ [\mathrm{mod}\,q])}{q} = \sum_{n=0}^{q-1}\frac{n}{q} = \frac{q.\,(q-1)}{2q} = \frac{q-1}{2}$$

Eventually, we can proove that :

$$\Gamma\left(1,\,\frac{p}{q}+r,\,0^+\right) = \frac{q+1}{2p} \qquad \Gamma\left(1,\,\frac{p}{q}+r,\,0^-\right) = \frac{q-1}{2p}$$

For the second case, we assume that α is irrationnal. So the sequence of $\mathrm{frac}\,(\alpha.n)_{n\in\mathbf{R}}$ is uniformly distributed and we have :

$$\lim_{N\to+\infty}\frac{1}{N}\sum_{n=0}^{N}\mathrm{frac}\,(\alpha n) = \frac{1}{2}$$

And then :

$$\forall\varphi\in\mathbf{R}\quad \Gamma(1,\,\alpha,\,\varphi) = \frac{1}{2\alpha}$$

References

[1] R. L. Rivest, *Illegitimi non carborundum*, Invited keynote talk given at CRYPTO 2011, August 15, 2011.

[2] M.van Dijk, A. Juels, A. Oprea, and R. L. Rivest, *FlipIt: The Game of "Stealthy Takeover"*, To appear in Journal of Cryptology, 2012.

[3] K. D. Bowers, M. van Dijk, R. Griffin, A. Juels, A. Oprea, R. L. Rivest, and N. Triandopoulos, *Defending against the Unknown Enemy: Applying FlipIt to System Security*, GameSec, 2012.